Datenschutz-Folgenabschätzung: Chancen, Grenzen, Umsetzung

Friedewald, Michael

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Friedewald, M. (2017). Datenschutz-Folgenabschätzung: Chancen, Grenzen, Umsetzung. *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis / Journal for Technology Assessment in Theory and Practice*, *26*(1-2), 66-71. https://doi.org/10.14512/tatup.26.1-2.66

Datenschutz-Folgenabschätzung

Chancen, Grenzen, Umsetzung

Michael Friedewald, *Fraunhofer-Institut für System- und Innovationsforschung, Breslauer Straße 48, 76139 Karlsruhe (michael.friedewald@isi.fraunhofer.de),* orcid.org/0000-0001-8295-9634

Mit der europäischen Datenschutz-Grundverordnung (DSGVO) besteht zum ersten Mal eine gesetzliche Verpflichtung für die Betreiber von Datenverarbeitung, in bestimmten Fällen eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. In diesem Beitrag wird erläutert, welche Anforderungen die DSGVO stellt und wie diese in einem modellhaften Prozess realisiert werden können. Ein besonderer Fokus liegt auf Elementen, die nach Erfahrung aus der TA-Tradition problematisch sein bzw. wie diese adressiert werden können.

Data Protection Impact Assessment
Opportunities, Barriers, Implementation

With the European General Data Protection Regulation (GDPR) there will be a legal obligation for controllers to conduct a Data Protection Impact Assessment (DPIA) for the first time. This paper examines the new provisions in detail and examines ways for their implementation. A special focus is on elements which, according to experience, can be problematic and how they can be addressed.

KEYWORDS: *data protection, privacy, fundamental rights, participation*

Von der Technikfolgenabschätzung zur Datenschutz-Folgenabschätzung

Technikfolgenabschätzungen haben eine jahrzehntelange Tradition. Sie dienen der Identifikation und Bewertung von technikinduzierten Auswirkungen auf Umwelt, Gesellschaft und Wirtschaft. Ziel ist der Gedanke der Vorsorge: Wie kann man bestehende oder zukünftige Risiken zuverlässig erkennen, eindämmen und beherrschen? Dabei dominierte in den 1970er- und frühen 1980er-Jahren vor allem die Betrachtung von Großtechnologien wie der Kernenergie. Seit Mitte der 1980er-Jahre sind auch Automation und elektronische Datenverarbeitung Themen der TA, allerdings zunächst mit Blick auf Veränderungen in der Arbeitswelt – Stichwort „menschenleere Fabrik" (Biervert und Monse 1990; U. S. Congress 1984).

https://doi.org/10.14512/tatup.26.1-2.66
Eingereicht: 14.3.2017. Angenommen: 27.4.2017

Nachdem das Konzept des Datenschutzes – zunächst als Gegengewicht gegen die staatliche „Datenmacht" – in der Nachfolge der (19)68er-Bewegung entwickelt wurde, das den Schutz der bürgerlichen Grundrechte zum Ziel hat (Lewinski 2012), wurde Datenschutz ab Mitte der 1980er-Jahre erstmals auch ein Gegenstand der TA (z. B. U. S. Congress 1985). Plädoyers für die Entwicklung einer rechtswissenschaftlichen Technikfolgenforschung (Roßnagel 1993) blieben allerdings zunächst folgenlos. Erst seit Beginn der 2000er-Jahre stehen Datenschutzaspekte verstärkt auch im Zentrum von TA-Studien (Klüver et al. 2006; Kündig und Bütschi 2008; Peissl 2007). Die meisten dieser Studien stellen fest, dass heutige Produkte und Dienstleistungen, die auf Vernetzung über das Internet und den Austausch von (häufig personenbezogenen) Daten basieren, zu einer Machtasymmetrie zwischen Anbietern und Nutzenden geführt haben, wobei letztere sich meist nur entscheiden können, ob sie die Angebote nach den Regeln der Anbieter oder gar nicht nutzen wollen. Daneben ist angesichts von zunehmenden Cyberattacken auf Internetdienste und deren Nutzer längst klar, dass Datenverarbeitung und Internet für das Funktionieren moderner Gesellschaft entscheidend sind und somit eine umfangreiche Technikfolgenabschätzung sinnvoll ist (Leimbach und Bachlechner 2014; Wanzeck 2008). Aus diesem Grund wurde in den entsprechenden TA-Studien gefordert, dass *Privacy Impact Assessments* (PIAs)[1] verpflichtender Bestandteil von IKT-Projekten sein sollten (Peissl 2007, S. 286).

PIAs werden im angelsächsischen Raum bereits seit Mitte der 1990er-Jahre diskutiert und teilweise auch durchgeführt. Allerdings verbergen sich dahinter weder eine einheitliche Methode noch einheitliche Anforderungen an die Umsetzung. Eine Verpflichtung zur Durchführung eines PIAs besteht ebenfalls meist nicht (zu Details Wright und De Hert 2012).

In der deutschen Gesetzgebung hatte die Technikfolgenabschätzung durchaus hoffnungsvoll begonnen, sie wurde aber durch verschiedene Gesetzgebungsnovellen bis zur Unkenntlichkeit verwässert (Friedewald et al. 2016, S. 8 f.). So ist zwar

1 Der Begriff Privacy Impact Assessment (für den es keine allgemein akzeptierte deutsche Übersetzung gibt) ist zumindest vor der Veröffentlichung des Entwurfs der DSGVO 2012 vielfach synonym mit dem der Datenschutz-Folgenabschätzung verwendet worden. Es gab aber zahlreiche Ansätze, auch Folgen jenseits des Datenschutzes zu bewerten und auch andere Grundrechte, soziale und ethische Folgen mit zu berücksichtigen (Wright und de Hert 2012, Part V).

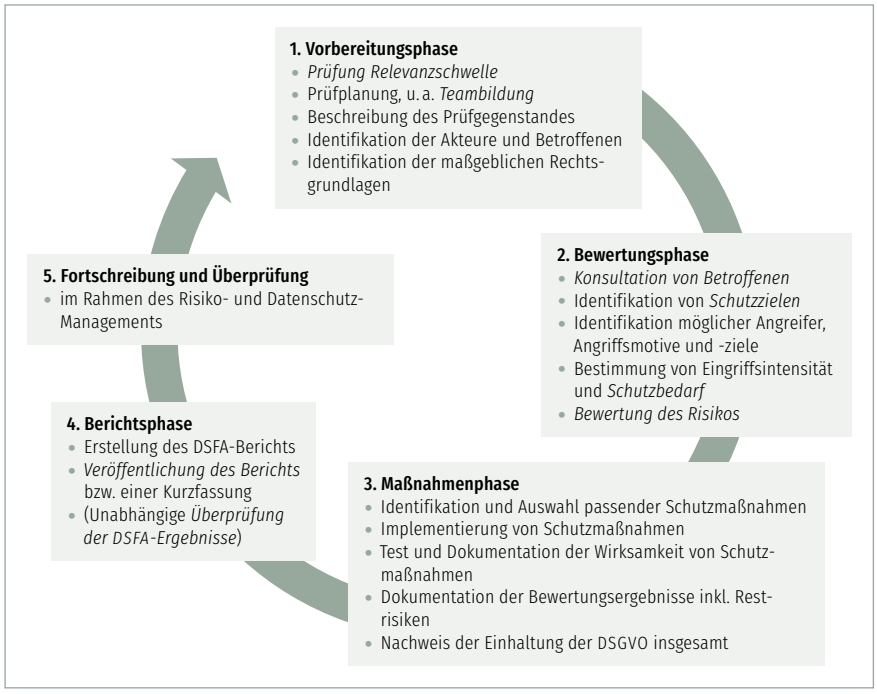

Abb. 1: Phasen einer Datenschutz-Folgenabschätzung. *Kursiv* gesetzte Prozesselemente werden im Text diskutiert. *Quelle: Eigene Darstellung*

in den noch geltenden Vorschriften des Bundesdatenschutzgesetzes eine Vorabkontrolle vorgesehen. Da aber jeder Betreiber nur für die Betrachtung der konkret von ihm durchgeführten Datenverarbeitungsvorgänge verpflichtet ist, bleiben insbesondere kumulative Wirkungen, die sich aus dem Zusammenspiel verschiedener Technologien ergeben können, außer Betracht (Le Grand und Barrau 2012). Vorgaben für eine standardisierte und unabhängige, nicht von Einzelinteressen geleitete Technikfolgenabschätzung fehlen vollständig.

Die Datenschutz-Folgenabschätzung nach der europäischen Datenschutz-Grundverordnung

Die ganze Situation ändert sich mit der europäischen Datenschutz-Grundverordnung (DSGVO), die ab 25. Mai 2018 angewendet wird. Sie hat als Verordnung grundsätzlich unmittelbar in allen Mitgliedstaaten Geltung und wird die Datenschutzrichtlinie aus dem Jahr 1995 (und deren nationale Umsetzungen) ersetzen. Ab diesem Zeitpunkt sind Organisationen und Unternehmen unter Androhung eines Bußgeldes verpflichtet, in bestimmten Fällen eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen.

Eine DSFA ist eine systematische Untersuchung eines Datenverarbeitungsverfahrens im Hinblick darauf, welche Risiken für den Datenschutz durch Organisationen (z. B. Unternehmen oder Behörden) aus der Perspektive der Betroffenen in verschiedenen Rollen und Kontexten (z. B. Bürger, Kunden, Patienten etc.) entstehen. Ziel der DSFA ist es, die Datenflüsse und Folgen der Datenverarbeitung so komplett wie nur möglich zu erfassen, sowie objektiv nach einheitlichen Kriterien so zu bewerten, dass typischen Risikoquellen mit adäquaten technischen und organisatorischen Gegenmaßnahmen begegnet und das Risiko für die Rechte der Betroffenen verringert werden kann (Friedewald et al. 2016, S. 5).

Über diesen Kernzweck hinaus können mit einer DSFA weitere Nebenziele verfolgt werden: Beispielsweise hilft die Durchführung einer DSFA Entwicklern dabei, Datenschutzrisiken zu erkennen und diese im Sinne des in Art. 25 DSGVO geforderten „Datenschutz durch Technikgestaltung" zu vermeiden. Gegenüber der Öffentlichkeit (inklusive der Politik) ist die DSFA ein Mittel zu Herstellung von Transparenz, die eine informierte Debatte über Risiken ermöglicht und Verantwortlichkeiten verdeutlicht.

Die DSGVO selbst definiert in Art. 35 Abs. 7 lediglich Mindestanforderungen an die Durchführung einer DSFA. Der Ausgangspunkt ist dabei eine systematische Beschreibung der vorgesehenen Verarbeitungsvorgänge und ihrer Zwecke (Art. 35 Abs. 7 lit. a DSGVO). Auf dieser Grundlage aufbauend können die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge sowie die Risiken für die Rechte der Betroffenen untersucht werden (Art. 35 Abs. 3 lit. b und c DSGVO). Schließlich muss jede DSFA erstens Abhilfemaßnahmen bezüglich der festgestellten Risiken benennen, diese verstehen sich einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren zum Schutz personenbezogener Daten. Zweitens muss jede DSFA nachweisen, dass die Bestimmungen der DSGVO insgesamt eingehalten werden (Art. 35 Abs. 3 lit. d DSGVO).

Abbildung 1 zeigt einen prototypischen Prozess, der die Bestimmungen der DSGVO erfüllt und Elemente kombiniert, mit denen in der Praxis die bestmöglichen Resultate erzielt werden können. Durch einen standardisierten Prozess wird die Reproduzierbarkeit und Überprüfbarkeit der Ergebnisse sichergestellt. So ist es für Dritte möglich, zu kontrollieren, ob rechtliche Vorgaben eingehalten werden. Es könnte Kunden bzw. Betroffene zudem in die Lage versetzen, die Datenschutzfolgen verschiedener technischer Systeme miteinander zu vergleichen. Schließlich fokussiert das Verfahren nicht nur auf eine Technologie oder Anwendung, sondern ist technologieneutral formuliert. Dies hilft, den Aufwand für die wiederholte Durchführung gering zu halten. Da die einzelnen Schritte bereits an anderer Stelle detailliert dokumentiert sind (Bieker et al. 2016; Friedewald et al. 2016), sollen im Folgenden einige entscheidende bzw. kritische Elemente diskutiert werden.

Wann ist eine Datenschutz-Folgenabschätzung durchzuführen?

Zunächst muss sich der Verantwortliche mit der Frage auseinandersetzen, ob im konkreten Fall die Durchführung einer DSFA überhaupt notwendig ist. Dies ist eine entscheidende, aber nicht triviale Frage, da die DSGVO in Art. 35 Abs. 1 bestimmt, dass eine DSFA durchzuführen ist, wenn „insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten" der Betroffenen besteht und dann in Art. 35 Abs. 3 ein nicht abschließender Katalog mit Anwendungsfällen aufgeführt wird. Zu diesen Anwendungsfällen mit hohem Risiko gehören: a) die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Profiling), b) die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten[2] oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie c) die systematische weiträumige Überwachung öffentlich zugänglicher Bereiche. Zusätzlich können die Aufsichtsbehörden nach Art. 35 Abs. 4–6 DSGVO weitere Anwendungsfälle definieren, in denen vorab eine DSFA vorzunehmen ist und solche, in denen keine DSFA notwendig ist.

Trotz einiger Hilfestellungen durch die Erwägungsgründe 75 und 76 bietet diese Bestimmung wegen der Verwendung von unbestimmten Begriffen („voraussichtlich … hohes Risiko") und nicht abschließenden Aufzählungen erheblichen Interpretationsspielraum. Aus diesem Grund hat die Artikel-29-Datenschutzgruppe (2017, S. 7 ff.) zehn Kriterien erarbeitet, nach denen sich eine Verarbeitung mit hohem Risiko bestimmen lässt. Dennoch besteht weiterhin erhebliche Unsicherheit, in welchen Fällen in der Praxis tatsächlich eine DSFA erforderlich ist. Die Einschätzung der Aufsichtsbehörden reicht momentan (Februar 2017) von „in wenigen Fällen" (CNIL, Frankreich) bis „sehr häufig" (ULD, Schleswig-Holstein). Es ist allerdings zu bedenken, dass die ernsthafte Feststellung, es bestehe kein „hohes Risiko", bereits eine Abschätzung potenzieller Folgen erfordert, die zu dokumentieren und ggf. einer Aufsichtsbehörde vorzulegen ist.

Es besteht weiterhin erhebliche Unsicherheit, in welchen Fällen in der Praxis tatsächlich eine DSFA erforderlich ist.

2 Hierzu gehören Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen bzw. Gewerkschaftszugehörigkeit sowie genetische, biometrische und Gesundheitsdaten sowie Daten über das Sexualleben und die sexuelle Orientierung.

Das DSFA-Team

Die Durchführung einer DSFA ist nach Art. 35 Abs. 1 eine Managementaufgabe, verantwortlich ist also die Unternehmens- oder Behördenleitung. Dies soll sicherstellen, dass sich die Datenschutz-Folgenabschätzung nicht anderen Zielen der Organisation unterzuordnen hat.

Die praktische Durchführung wird in der Regel an Mitarbeiter oder einen externen Dienstleister delegiert werden. Nach Art. 35 Abs. 2 ist dabei (sofern vorhanden) der Rat des betrieblichen oder behördlichen Datenschutzbeauftragten (bDSB) einzuholen. Offen bleibt, wie die konkrete Beteiligung des bDSB aussehen soll. Insbesondere bei kleinen Organisationen ist es naheliegend, wenn der Verantwortliche den bDSB mit der Koordination oder Durchführung der DSFA beauftragt, da dieser in der Regel die dafür erforderliche fachliche Eignung hat. Mit Hinweis auf die Weisungsunabhängigkeit des bDSB kann man aber durchaus auch die Meinung vertreten, dass der bDSB lediglich die Durchführung mit Ratschlägen begleiten bzw. überwachen sollte – so auch die Position der Artikel-29-Datenschutzgruppe (2016, S. 16 f.).

Unübersehbar ist aber ein zentraler Interessenskonflikt: Die Organisation soll einerseits die Datenschutzrisiken möglichst umfassend und im Sinne der Betroffenen beurteilen, sie hat aber gleichzeitig u. U. ein Interesse daran, personenbezogene Daten für eigene Partikularinteressen zu nutzen. Um auszuschließen, dass sich die Organisation bei der Analyse als mögliche Risikoquelle ausblendet, sollte wenigstens eine nachträgliche Überprüfung durchgeführt werden. Bei der Zusammenstellung des Teams ist es wichtig, eine Balance zwischen Unabhängigkeit und Verantwortlichkeit herzustellen. Für die Objektivität und Glaubwürdigkeit der Ergebnisse ist entscheidend, dass das Team in der Lage ist, eine wirkungsvolle Prüfung vorzunehmen. Darüber hinaus ist eine ausreichende Berücksichtigung der Interessen aller Betroffenen sicherzustellen (s. u.). Auch vom bDSB (sofern ein solcher benannt ist) ist zu erwarten, dass er die Betroffenenperspektive einnimmt und seine eigene Organisation „von außen" betrachtet.

Konsultation von Betroffenen

Da es im bisherigen Datenschutzrecht letztlich um die Sicherstellung individueller Rechte jedes Einzelnen geht, fordern wissenschaftliche Studien bereits seit Jahren, dass bei Datenschutz-Folgenabschätzungen (bzw. PIAs) nicht nur die Sicht von (technischen und juristischen) Experten eingeholt werden sollte. Mit der elaborierten Expertise technischer Experten allein geht nämlich die Gefahr einer verengten Sichtweise und folglich einer technokratisch-paternalistischen Bevormundung Technik nutzender Personen einher. Vielmehr sei eine umfassende und thematisch breite Konsultation der Betroffenen notwendig. Dabei sollte aber die Frage im Blick behalten werden, welche Akteure überhaupt als „relevant" gelten und wer darüber entscheidet (Wright und Friedewald 2013; Wright et al. 2015). Diesen Überlegungen trägt auch Art. 35 Abs. 9 DSGVO Rechnung, der vorsieht, dass für eine DSFA der Standpunkt der betroffenen Per-

sonen eingeholt werden soll. Allerdings wird diese Vorschrift insofern relativiert, als zum Schutz gewerblicher oder öffentlicher Interessen auch auf die Konsultation verzichtet werden kann.

Unbeschadet solcher Einschränkungen stellt sich die Frage, auf welche Weise die verschiedenen Akteursgruppen und Interessen im Bewertungsprozess einer Datenschutz-Folgenabschätzung eingebunden werden können. Methodisch bieten sich hierbei relativ einfache und bewährte Verfahren an, mit denen Unternehmen bereits in den Bereichen Produktgestaltung und Marketing Erfahrung haben (z. B. Fokusgruppen), aber natürlich sind auch elaboriertere pTA-Methoden einsetzbar.

Eine Bewertung unter Mitwirkung von Betroffenen stellt allerdings besondere Herausforderungen an Zeitpunkt und Umstände:

- Bei einer DSFA, die vor der Markteinführung bzw. parallel zum Entwicklungsprozess durchgeführt wird, kann die Einbeziehung von externen, u. U. kritisch eingestellten Personengruppen unerwünscht sein, nicht nur weil Betriebs- und Geschäftsgeheimnisse betroffen sind, sondern auch weil aus Imagegründen keine unausgereiften Lösungen präsentiert werden sollen.
- Die Einbeziehung von Betroffenen kann problematisch sein, da eine sorgfältige und systematische Bewertung häufig Fachwissen erfordert, das bei technischen Laien nicht vorausgesetzt werden kann. Hier ist somit die Frage maßgeblich, wie sich dieses Fachwissen vermitteln lässt, damit eine Diskussion „auf Augenhöhe" zwischen Laien und Experten möglich ist.
- Das für das Bewertungsverfahren verwendete Vokabular hat Folgen für die Intensität und Qualität der Einbeziehung unterschiedlicher Akteursgruppen. So dürften bestimmte Formulierungsweisen etwa besonders technophile Akteure oder solche mit Rechtskenntnissen begünstigen. Fraglich ist daher, wie sich Übersetzungsprozesse zwischen den beteiligten Gruppen erfolgreich gestalten lassen.

Umfangreiche partizipative DSFAen unter Einbeziehung von Externen werden vermutlich schon deswegen eher die Ausnahme bleiben, da dieser Prozess zeitaufwendiger ist und es ansonsten bei bestimmten Akteursgruppen rasch zu einer „Konsultationsmüdigkeit" kommen könnte. Im Normalfall ist aber zumindest darauf zu achten, auch solche Gruppen innerhalb einer Organisation mit einzubinden, die unmittelbar mit den Betroffenen zu tun haben, also Verkauf oder Service bzw. der Betriebs- oder Personalrat (Kiesche 2017).

Bewertungsphase

Die Anforderungen des Datenschutzes sind gesetzlich vorgeschrieben. Diese Anforderungen lassen sich mit Hilfe von sog. Gewährleistungszielen umsetzen, die in kompakter und methodisch zugänglicher Form die operativen Risiken explizit machen, vor denen es durch angemessene Verfahrensgestaltung und Maßnahmen zu schützen gilt. Sechs Gewährleistungsziele gelten derzeit im Bereich des Datenschutzes als etabliert. Den Risiken der Informationssicherheit wird klassisch mit der Sicherung der drei Schutzziele (1) Verfügbarkeit, (2) Integrität und (3) Vertraulichkeit begegnet. Aufbauend hierauf werden zusätzlich als spezifische Datenschutzschutzziele formuliert: (4) Nichtverkettbarkeit, (5) Transparenz und (6) Intervenierbarkeit (für Details Rost und Bock 2011; Rost und Pfitzmann 2009). Als zusätzliches Schutzziel nennt die DSGVO die Belastbarkeit (im englischen Text der DSGVO: *resilience*) der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO). Für die Bewertung eines Risikos haben sich die Schutzbedarfsabstufungen (normal, hoch, sehr hoch) bewährt, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinen IT-Grundschutz-Katalogen empfiehlt.

Die eigentliche Herausforderung liegt freilich darin, dass bei dem auf Grundrechtsschutz angelegten Datenschutz der Schutzbedarf nicht wie beim Risikomanagement allein anhand von Schadenshöhen und Eintrittswahrscheinlichkeiten bestimmt werden darf, obwohl Art. 24 Abs. 1 DSGVO vorschreibt, dass der Verantwortliche genau diese Größen bei der Auswahl und Implementierung von technisch-organisatorischen Maßnahmen berücksichtigen soll. Darüber hinaus gibt es aus rein praktischen Erwägungen Unsicherheit, welche Form der Bewertung Unternehmen und Behörden zuzumuten sind. Eine Checkliste, auf der (wie bei der bisherigen Vorabkontrolle) kritische Punkte bzw. Schutzmaßnahmen abgehakt werden, ist zwar einfach einzusetzen, wird aber der Komplexität moderner IT-Systeme meist nicht gerecht und führt auch nicht zu einer ausreichenden Auseinandersetzung der Verantwortlichen mit möglichen Gefahren für den Datenschutz. Andererseits ist ein auf Datenschutz angepasstes Risikomanagement in Anlehnung an ISO 31 000, wie es beispielsweise von der französischen Datenschutzaufsicht (CNIL 2015) propagiert wird, für viele kleinere und mittlere Unternehmen, Freiberufler und Behörden in der Praxis oft zu voraussetzungsvoll und umfangreich.

Hierzu besteht deshalb noch Forschungs- und Normierungsbedarf, um *alle* Verantwortlichen in die Lage zu versetzen, eine aussagekräftige und damit zweckmäßige DSFA zu erstellen. Das Standard-Datenschutzmodell der Konferenz der unabhängigen

In der deutschen Datenschutz-Gesetzgebung hatte die Technikfolgenabschätzung durchaus hoffnungsvoll begonnen, sie wurde aber durch verschiedene Gesetzgebungsnovellen bis zur Unkenntlichkeit verwässert.

Datenschutzbehörden des Bundes und der Länder[3] ist ein erfolgversprechender Ansatz in dieser Richtung, der 2017/18 in einem vom Autor geleiteten Forschungsprojekt weiterentwickelt und praktisch getestet wird.

Berichtsphase

Ein DSFA-Bericht sollte im Sinne der Transparenz veröffentlicht werden, zumindest in einer Kurzversion, die Geschäftsgeheimnisse sowie die Restrisikoanalyse, die sonst als Angriffsvorlage missbraucht werden könnte, ausspart. Es sollten aber alle wesentlichen Informationen enthalten sein und keine (negativen) Ergebnisse der Untersuchung verschwiegen werden. Allerdings ist eine Veröffentlichung der DSFA-Ergebnisse nach der DSGVO nicht verpflichtend vorgeschrieben, wird aber von der Artikel-29-Datenschutzgruppe (2017, S. 17) empfohlen.

Um zu gewährleisten, dass die DSFA ordnungsgemäß durchgeführt wurde, ist es sinnvoll, die DSFA von einem unabhängigen Dritten, einem externen Auditor oder der zuständigen Datenschutzaufsichtsbehörde überprüfen zu lassen. Die Überprüfung sollte insbesondere sicherstellen, dass angemessen mit Interessenskonflikten umgegangen wurde, die Interessen der Betroffenen angemessen berücksichtigt wurden, die Öffentlichkeit ausreichend über die Ergebnisse der DSFA informiert wird und die vorgeschlagenen Schutzmaßnahmen tatsächlich umgesetzt wurden. Dies könnte dann Grundlage der in Art. 42 DSGVO vorgesehenen Zertifizierung oder eines Datenschutzsiegels sein.

Fortschreibung

Die Abschätzung von Datenschutzfolgen ist kein einmaliger und linearer Prozess, sondern muss während des gesamten Lebenszyklus eines Projekts fortlaufend überwacht werden. Der Grund hierfür liegt im bekannten Steuerungs- oder Collingridge-Dilemma (Grunwald 2010, S. 165 ff.). Kern dieses Dilemmas ist die Forderung, dass eine Folgenabschätzung möglichst frühzeitig erfolgen sollte, um noch Änderungen in der Gestaltung vornehmen zu können. Gleichzeitig ist es aber notwendig, die zu bewertende Technologie oder den zu bewertenden Prozess so genau wie möglich zu beschreiben und zu charakterisieren, was erst in späteren Entwicklungsphasen möglich ist, wenn grundsätzliche Gestaltungsentscheidungen längst gefallen sind und nicht mehr ohne Weiteres geändert werden können.

Art. 35 Abs. 11 DSGVO legt fest, dass die DSFA jedenfalls dann zu wiederholen ist, wenn sich das mit der Verarbeitung verbundene Risiko ändert. Die Artikel-29-Datenschutzgruppe (2017, S. 12) empfiehlt darüber hinaus, dass wenigstens alle drei Jahre überprüft werden sollte, ob die Ergebnisse einer DSFA noch zutreffend sind. Insofern hat der Verantwortliche kontinuierlich zu überwachen, ob sich die Rahmenbedingungen des Einsatzes in technischen, organisatorischen oder rechtlichen Weisen ändern, die neue Datenschutzrisiken nach sich ziehen. Auch hat er zu überwachen, ob die gewählten Schutzmaßnahmen den erwarteten Nutzen haben. Es gilt sicherzustellen, dass die Maßnahmen an Veränderungen angepasst werden. Um auf Veränderungen der Rahmenbedingungen möglichst effizient reagieren zu können, ist eine Einbindung in das allgemeine Risiko- und/oder Datenschutz-Management der Organisation ratsam (Rost 2013; Wright et al. 2014).

Fazit

Die Datenschutz-Folgenabschätzung ist in den meisten EU-Mitgliedstaaten ein relativ neues Instrument zur Identifikation von Risiken, die durch den Einsatz von (neuen) datenverarbeitenden Technologien und Systemen für die Grundrechte der Menschen auf Achtung des Privatlebens und den Schutz personenbezogener Daten entstehen. Sie hat Potenzial als „Frühwarnsystem", das es den beteiligten Akteuren erlaubt, über die Folgen technischer Entwicklungen und deren Nutzung systematisch nachzudenken sowie mögliche Mängel rechtzeitig – idealerweise bereits in der Entwurfsphase eines Systems – zu erkennen und zu beseitigen. Ein Fortschritt gegenüber früheren Ansätzen ist dabei der Rückgriff auf eine Reihe von standardisierten Bewertungskriterien: Diese gewährleisten, dass Betroffenenrechte umfassend betrachtet werden und garantieren gleichzeitig die Vergleichbarkeit. Damit kann eine in der Technikfolgenabschätzung häufig vermisste Balance zwischen dem Verlangen nach Normativität auf der einen und nach Operationalisierung auf der anderen Seite hergestellt werden.

Unverkennbar ist aber auch, dass es für die praktische Umsetzung noch eine ganze Reihe methodisch-praktischer Fragen zu klären gilt, insbesondere bezüglich der systematischen und aktiven Konsultation der Betroffenen. Darüber hinaus sind noch Wege zu eruieren, wie man mit dem Problem umgehen soll, dass die Risikoabschätzung durch den potenziellen Verursacher des Risikos selbst erfolgt. Hier besteht freilich die Hoffnung, dass sich die Erfahrungen aus mehreren Jahrzehnten praktischer Technikfolgenabschätzung für diesen Bereich fruchtbar machen lassen.

Allerdings blenden die Vorschriften der DSGVO auch wichtige Aspekte aus, die für eine umfassende Folgenabschätzung wünschenswert wären. Dies ist einerseits die Limitierung auf Folgen für das Individuum, da mittlerweile auch das Recht von Gruppen und Institutionen auf Datenschutz zunehmend als wichtig erachtet wird (Taylor et al. 2017). Im Sinne einer stärker ganzheitlichen Bewertung von Technikfolgen wäre andererseits eine Erweiterung auf weitere Rechte und Freiheiten (Recht auf Schutz des Privatlebens, Meinungsfreiheit, Benachteiligungsverbot etc.) und die Kombination mit anderen Bewertungsdimensionen (sozial, ethisch etc.) wünschenswert.

Insgesamt bietet die Verpflichtung zur Durchführung von DSFAen für die Technikfolgenabschätzung die Chance, rechtliche Technikfolgen (wieder) stärker zu adressieren, so wie es auch im Rahmen von Responsible Research and Innovation vorgeschlagen wird (Schomberg 2011).

3 https://www.datenschutzzentrum.de/sdm/

Literatur

Artikel-29-Datenschutzgruppe (2016). Guidelines on Data Protection Officers (DPOs). 16/EN, WP 243. Brüssel. Online verfügbar unter http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf, zuletzt geprüft am 13. 6. 2017.

Artikel-29-Datenschutzgruppe (2017): Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "Likely to Result in a High Risk„ for the Purposes of Regulation 2016/679. 17/EN, WP 248. Brüssel. Online verfügbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, zuletzt geprüft am 13. 6. 2017.

Bieker, Felix; Hansen, Marit; Friedewald, Michael (2016): Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung. In: RDV – Recht der Datenverarbeitung 32 (4), S. 188–197.

Biervert, Bernd; Monse, Kurt (1990): Technik und Alltag – Mittelbare und unmittelbare Wirkungen der neuen Informations- und Kommunikationstechniken für die privaten Haushalte. In: Kistler, Ernst; Jaufmann, Dieter (Hg.): Mensch – Gesellschaft – Technik: Orientierungspunkte in der Technikakzeptanzdebatte. Opladen: Leske + Budrich, S. 195–213.

CNIL (Commission Nationale de l'Informatique et des Libertés) (2015): Privacy Risk Assessment: Methodology (How to Carry Out a PIA). Paris. Online verfügbar unter http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf, zuletzt geprüft am 13. 6. 2017.

Friedewald, Michael; Obersteller, Hannah; Nebel, Maxi et al. (2016): Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. White Paper. Karlsruhe: Fraunhofer ISI. Online verfügbar unter https://datenschutzzentrum.de/artikel/1018-.html, zuletzt geprüft am 13. 6. 2017.

Grunwald, Armin (2010): Technikfolgenabschätzung – eine Einführung. 2. Aufl. Berlin: Edition Sigma.

Kiesche, Eberhard (2017): So funktioniert die Folgenabschätzung. In: Computer und Arbeit 26 (2), S. 31–36.

Klüver, Lars; Berloznik, Robby; Peissl, Walter; Tennøe, Tore; Cope, David; Belluci, Sergio (2006): ICT and Privacy in Europe: Experiences from Technology Assessment of ICT and Privacy in Seven Different European Countries. Online verfügbar unter https://teknologiradet.no/wp-content/uploads/sites/19/2013/08/Rapport-ICT-and-Privacy-in-Europe.pdf, zuletzt geprüft am 13. 6. 2017.

Kündig, Albert; Bütschi, Danielle (Hg.) (2008): Die Verselbständigung des Computers. Zürich: vdf Hochschulverlag.

Le Grand, Gwendal; Barrau, Emilie (2012): Prior Checking, a Forerunner to Privacy Impact Assessments. In: Wright, David; De Hert, Paul (Hg.): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer, S. 97–116.

Leimbach, Timo; Bachlechner, Daniel (2014): Big Data in der Cloud. TA-Vorstudie. Hintergrundpapier 19. Berlin: Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag.

Lewinski, Kai von (2012): Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive. In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hg.): Datenschutz: Grundlagen, Entwicklungen und Kontroversen. Bonn: Bundeszentrale für politische Bildung, S. 23–33.

Peissl, Walter (2007): Die Bedrohung von Privacy: Ein grenzüberschreitendes Phänomen und seine Behandlung im Kontext internationaler Technikfolgenabschätzung. In: Bora, Alfons; Bröchler, Stephan; Decker, Michael (Hg.): Technology Assessment in der Weltgesellschaft. Berlin: Edition Sigma, S. 277–288.

Roßnagel, Alexander (1993): Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin. Baden-Baden: Nomos.

Rost, Martin (2013): Datenschutzmanagementsystem. In: DuD – Datenschutz und Datensicherheit 37 (5), S. 295–300.

Rost, Martin; Bock, Kirsten (2011): Privacy by Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen. In: DuD – Datenschutz und Datensicherheit 35 (1), S. 30–35.

Rost, Martin; Pfitzmann, Andreas (2009): Datenschutz-Schutzziele – revisited. In: DuD – Datenschutz und Datensicherheit 33 (6), S. 353–358.

Schomberg, René von (2011): Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. In: René von Schomberg (Hg.): Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Luxembourg: Publications Office of the European Union, S. 7–15.

Taylor, Linnet; Floridi, Luciano; van der Sloot, Bart (Hg.) (2017): Group Privacy: New Challenges of Data Technologies. Cham: Springer.

U. S. Congress, Office of Technology Assessment (1984). Computerized Manufacturing Automation: Employment, Education, and the Workplace. OTA- CIT-235. Washington, D. C.: U. S. Government Printing Office.

U. S. Congress, Office of Technology Assessment (1985). Electronic Surveillance and Civil Liberties. OTA-CIT-293. Washington, D. C.: U. S. Government Printing Office.

Wanzeck, Markus (2008): Datenverarbeitung ist Risikotechnologie (Interview mit Ralf Bendrath). In: Stern vom 24. August 2008. Online verfügbar unter http://www.stern.de/digital/computer/interview-ralf-bendrath--datenverarbeitung-ist-risikotechnologie--3753036.html, zuletzt geprüft am 26. 4. 2017.

Wright, David; De Hert, Paul (Hg.) (2012): Privacy Impact Assessment. Dordrecht, Heidelberg, London, New York: Springer.

Wright, David; Friedewald, Michael (2013): Integrating Privacy and Ethical Impact Assessment. In: Science and public policy 40 (6), S. 755–766.

Wright, David; Friedewald, Michael; Gellert, Raphaël (2015): Developing and Testing a Surveillance Impact Assessment Methodology. In: International Data Privacy Law 5 (1), S. 40–53.

Wright, David; Wadhwa, Kush; Lagazio, Monica; Raab Charles; Charikane, Eric (2014): Integrating Privacy Impact Assessment in Risk Management. In: International Data Privacy Law 4 (2), S. 155–170.

DR. MICHAEL FRIEDEWALD

leitet das Geschäftsfeld Informations- und Kommunikationstechnik am Fraunhofer-Institut für System- und Innovationsforschung in Karlsruhe. Zu seinen Arbeitsschwerpunkten gehört die Bewertung von Auswirkungen neuer IKT-Technologien auf Privatheit und Datenschutz.